State of California
Office of the State Chief Information Officer
Office of Technology Services

Procedure

Owner: Security Management Division

Number: 3502
Issue Date: 05/12/2008
Revised: 11/16/2009

INFORMATION SECURITY EXCEPTION REQUEST

Section 1 – Introduction

The Security Management Division (SMD) has published five Office of the State Chief Information Officer (OCIO), Office of Technology Services (OTech) Information Security Policies and multiple supporting security standard and procedures to ensure a safe and secure working environment for its customers, visitors, and employees. These Security Policies and Procedures were written to directly reflect the position of the OTech Information Security Office (ISO); they should be adhered to by customers, visitors, and employees. The SMD is aware that exceptions can occur from time to time. This Procedure explains the exception request procedure for an SMD Policy or Procedure.

Section 2 – Exception Request Procedure

A. Exception Qualification

The exception request procedure should be followed if either of the criteria below applies.

1. The Security Policy or Procedure in question cannot be adhered to for unforeseen reasons outside of your control.
2. In working closely with the SMD, alternative solutions have been exhausted and are not possible.

B. Exception Request Procedure

Information Security Policy or Procedure exception requests must be linked to an existing Service Request. The following procedure begins when a customer or employee has an exception request to a published Security Policy or Procedure:

1. An SMD representative provides risk assessment and alternative recommendations to the requester's ISO; doing so may involve more OTech subject matter experts.
2. The requester's ISO either accepts or declines the assessment and alternative recommendations.
    a. If the requester's ISO accepts, the SMD works with the customer to re-architect the issue to mitigate security risk(s). The exception is terminated and efforts continue.
    b. If the requester's ISO declines, the requester must complete the Security Policy/Procedure Exception Request Form, OCIO 358. The SMD manages the form and will place a reference in the corresponding Service Request.
3. The SMD will conduct meetings with the OTech ISO to discuss the request background, documentation, risk assessment and recommended alternative.
4. The OTech ISO either accepts or declines the exception request.

a. If the OTech ISO accepts the request, SMD staff document responses from the requester and OTech ISO thus far. SMD will send copies of the findings to the requester's ISO. The exception request is approved, the exception is implemented.
b. If the OTech ISO declines the request, SMD staff drafts and sends a formal exception denial letter to the requester's ISO. SMD staff continues to work with the requester until an acceptable solution can be agreed upon. The exception terminates, and documentation is filed and noted in the Service Request.

Section 3 – Applicability and Exclusions

A. This Procedure applies to customers and employees. Direct any questions regarding the applicability of this Procedure to the SMD for clarification.

B. Exceptions will be considered on a case-by-case basis. Requests for an exception to a Security Policy or Procedure must be submitted to the SMD via the OTech Security Policy/Procedure Exception Request Form, OCIO 358.

Section 4 – Auditing and Reporting

A. Information security exception requests must be tied to a Service Request for tracking.

B. Auditing may be performed on a periodic or random basis by the SMD or its designees. In the event an audit determines this Procedure is not being applied, notification will be sent to the appropriate person for remediation.

C. Any known violations of this Procedure must be reported to the OTech ISO and the reporting employee's immediate supervisor.

Section 5 – Authority/References

Security Policy/Procedure Exception Request Form, OCIO 358

Please contact your OTech Customer Representative to review the following:

3500 – Security Awareness Policy